ABSTRACT OF THE DISCLOSURE

Access control approaches are disclosed wherein managed object in Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) are accessed on a per-Virtual Private Network (VPN)-basis with no modifications to existing MIBs. A manager and an SNMP Agent operating in a VPN environment agree on a mapping between SNMP securityNames and VPN IDs. Under the agreed mapping, the target VPN of any SNMP management request can be unambiguously determined from the securityName alone. For each securityName, one or more MIB Views are configured using in a View-based Access Control Model MIB (VACM MIB) table; the MIB Views specify which portions of the managed object tree can be viewed or modified by a corresponding VPN. Thereafter, a VPN-enabled device provides SNMP requests in which a VPN ID value is passed in the securityName field of the context string in the community string. The receiving device extracts the securityName, locates corresponding MIB Views using the VACM MIB table, and allows the requesting device to access only objects that are identified in the MIB Views.